



Firmware Release Note

P-334WT

Release 3.60(JN.8)C0

| | |
|----------------|---------------------|
| Date: | Oct 05, 2005 |
| Author: | Brian Chang |

ZyXEL P-334WT Standard Version release 3.60(JN.8)C0 Release Note

Date: Oct 05, 2005

Supported Platforms:

ZyXEL P-334WT

Versions:

ZyNOS Version: V3.60(JN.8) | 10/05/2005 09:33:12

Bootbase Version: V1.05 | 04/20/2004 10:36:26

Notes:

1. This version supports quick route and enabled by default.
2. If Wireless Port Control (SMT Menu 23.4) is "Authentication Required", P334WT will enable 802.1x/WPA/WPA-PSK user authentication mechanism, a wireless user must login the P334WT successfully before accessing network service. If Wireless Port Control is "No Authentication Required", P334WT will allow all wireless users to access network service. If Wireless Port Control is "No Access Allowed", P334WT will not allow wireless user to access network service.
3. The first entry of static route is reserved for system and read-only for users.
4. External Help Pages.

Known Issues:

1. The device fails to add a firewall ACL rule for NAT server set #12 automatically.
2. Allow NetBIOS traffic between WAN & LAN doesn't work when Firewall is enabled.
3. Computers using Any IP need clear ARP table to access network after P334WT reboot.
4. Into SMT 21.1.1.1 TCP/IP Filter rule, save source and destination IP address then back to configure again would show the error message and can not save.
5. Using FTP to upgrade F/W may cause system hang sometimes and need to reboot by manual.
6. Interoperability problem with Netgear stations MA401 and MA111 when configured in short preamble. For this issue, user must change to long preamble.
7. The Trend Micro Security Services Web page may not appear if you are using instant messaging software other than MSN Messenger (for example, ICQ) or you have installed software that blocks popup browser windows (for example, the

Google toolbar or Windows XP Service Pack 2). User must either disable the SP2 pop-up blocker temporarily or type the <http://tmss.trendmicro.com/dashboard> to access the TMSS Dashboard installation process manually. Once the TMSS ActiveX control has been installed, user can easily access the Dashboard by either clicking the IE toolbar TMSS icon or launch the "Trend Micro Security Services" from the Start menu.

8. Enable traffic redirect under PPTP encapsulation and DHCP set none, traffic goes out via traffic redirect but not via WAN.
9. When WAN line is attached, PPPoE dynamic connection can't be built successfully via Wizard.

CI Command List:

Features:

Modification in 3.60(JN.8)C0 | 10/05/2005

1. Change 3.60(JN.8)b1 to 3.60(JN.8)C0 FCS version.

Modification in 3.60(JN.8)b1 | 09/26/2005

1. [BUG FIXED]
Symptom: MBM downloads are seriously affected by simultaneous uploads traffic.
Condition: Enable MBM, doing FTP download and inject heavy upload traffic will cause FTP download almost stop.
2. [BUG FIXED]
Symptom: Device learns wrong ARP rule and causes LAN work fail.
Condition:
 - 1) Device connects to Internet via PPPoE Server
 - 2) Device DHCP Server automatically assigns one IP Address for client in LAN side.
 - 3) Client gets IP Address 192.168.1.2 from device.
 - 4) Device shows arp status 192.168.1.2 be enif0 (LAN side)
 - 5) Client can connect to Internet
 - 6) Set one WAN side PC's IP as the same as client's IP (192.168.1.2)
 - 7) WAN side PC ping 192.168.1.1 (Device's LAN IP)
 - 8) Device shows that arp status 192.168.1.2 be enif1
 - 9) LAN side client can't access to Internet.

Modification in 3.60(JN.7)C0 | 07/25/2005

1. Change 3.60(JN.6)b5 to 3.60(JN.7)C0 FCS version.

Modification in 3.60(JN.6)b4 | 07/12/2005

1. [BUG FIXED]
SPR: 050708499
Symptom: Traceroute will fail under Linux O.S

ZyXEL Confidential

Condition:

- 1) Turn on Firewall
- 2) Linux computer locates in LAN side and traceroute to the host which distance is over 5 hubs.
- 3) Firewall judges that Linux traceroute behavior is port scan attack

Modification in 3.60(JN.6)b3 | 07/04/2005

1. [BUG FIXED]
SPR: 050627332
Symptom: Some filed is dropped by upgrade firmware
Condition:
 - 1).Upgrade from version 3.60(JN.4) to version 3.60(JN.6)b2
 - 2).The Authentication Server IP Address and Shared Secret, and the Accounting Server IP Address and Shared Secret were dropped.
 - 3).The fields were empty after the upgrade
2. [BUG FIXED]
SPR: 050602130
Symptom: Device will show error message on UI.
Condition: Press two times of Apply button when setting WLAN OTIST page, device will display error message on UI.
3. [BUG FIXED]
Symptom: Device didn't use user-defined server to sync correct time.
Condition: Input a NTP server address and save it at eWC, then check information at Logs page will see device use default built-in server to get current time.
4. [BUG FIXED]
SPR: 050627330
Symptom: Host can't login DUT GUI after another host logout.
5. [BUG FIXED]
SPR: 050620783
Symptom: Filter function shows wrong information.
Condition:
 - 1). Execute connection wizard at eWC.
 - 2). Then go to SMT menu 11.5 will see wrong filter settings as 1,1,1,1
6. [BUG FIXED]
SPR: 050627334
Symptom: WLAN status Encryption is not consist with WLAN setting.
Condition: Change "Encryption" to "Security mode" on Status page.
7. [FEATURE ENHANCED]
SPR: 050627335
Symptom: The information is not clearly at Password Page.
Condition: Change as "Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2".
8. [FEATURE ENHANCED]
SPR: 050627336
Symptom: Change word to capital in the opening sentence at "Please select Wizard or Advanced mode".

ZyXEL Confidential

9. [FEATURE CHANGED]
SPR: 050627333, 050627339
Symptom: Remove firewall note on Remote Management screens.
10. [FEATURE ENHANCED]
SPR: 050627344
Symptom: Change the sentence as following on Network/Wireless LAN/OTIST:
“Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience”
Condition: Only change on English version.
11. [FEATURE ENHANCED]
SPR: 050627337
Symptom: “connection wizard” should be capitalized in the opening sentence for consistency.
12. [FEATURE ENHANCED]
SPR: 050627338
Symptom: Sentence on OTIST Wizard Page is not correct. “This key should not be the same as the router password the password you use to log in to your ISP”.
Condition: This sentence is un-necessary, remove it.

Modification in 3.60(JN.6)b2 | 06/14/2005

1. [BUG FIXED]
SPR: 050602123, 050602124
Symptom: WPA2 mixed mode can't work fine with Centrino 2200BG.
Condition:
 - 1). Setup WPA2 mixed mode environment (re-authentication timer=120seconds, update group key timer=60 seconds)
 - 2). Use two wireless STA (G-162, Centrino 2200BG) to associate to P-33WT
 - 3). If Centrino use WPA2 to associate to P-334WT, then Centrino can not pass authentication process after 120 seconds. (But we click the re-connect, then Centrino can associate to it)
 - 4). If Centrino use WPA to associate to P-334WT, then Centrino will reconnect to P-334WT after 240 seconds.
2. [BUG FIXED]
SPR: 050607393
Symptom: STA will disconnect under stress test.
Condition:
 - 1). Setup WPA2_PSK mixed mode in AP.
 - 2). prepare 7 wireless STA (Centrino B, Centrino B/G, Sonoma A/B/G, D-link DWL G-122, G-220, NEC G-100, G-162) to associate to P-334WT.
 - 3). P-334WT show "Recovery: Full time mediem usage" after overnight stress testing.
3. [BUG FIXED]
SPR: 050602132
Symptom: Cisco AIR-CB21AG-W-K9 throughput test unstable.

ZyXEL Confidential

4. [BUG FIXED]
SPR: 050602122
Symptom: WPA mode can't work fine
Condition: Setup WPA_PSK, then change to WPA and modify RADIUS IP and shared secret key. STA can't connect to device unless reboot the device.
5. [BUG FIXED]
SPR: 050603181
Symptom: Configure QoS page cause device crash.
Condition: Configure name to 8 characters for two rules, device will crash.
6. [BUG FIXED]
SPR: 050606291
Symptom: Device exception when setup VPN manual mode.
Condition: When change VPN IKE to Manual mode and try to establish the tunnel, device will crash.
7. [BUG FIXED]
SPR: 050607397
Symptom: Parental Control should be disabled when user doesn't get the license.
8. [BUG FIXED]
SPR: 050607398
Symptom: Parental Control can't work fine when select match categories.
9. [BUG FIXED]
SPR: 050609480
Symptom: System time can't sync with Time Server when enable daylight saving.
10. [BUG FIXED]
SPR: 050531904
Symptom: SMT menu will show some garbage.
Condition:
 - 1). In menu3.2: setting DHCP type= Server, Third DNS Server= User-Defined
 - 2). then change the DHCP type to Relay or None, the line of Third DNS Server still keep some characters "ned".

Modification in 3.60(JN.6)b1 | 05/29/2005

1. [FEATURE ENHANCED]
Symptom: Support WiFi WPA2
2. [FEATURE ENHANCED]
Symptom: Support WiFi WMM
3. [FEATURE ENHANCED]
Symptom: Support new GUI
4. [FEATURE ENHANCED]
Symptom: Changing the format of daylight saving to correspond with the popular configuration.
Condition:

| | |
|-------------|---|
| old config: | start month - day |
| | end month - day |
| new config: | start month - nth week - weekday - hour |

end month - nth week - weekday - hour

5. [BUG FIXED]
SPR: 050121234
Symptom: P334WT deployment issue.
Condition:
Step1: PC1----P334WT----ZW5----P334----PC2(P334 & P334WT are under LAN side of ZW5)
Step2: PC2----P334WT----ZW5----P334----PC1(P334 & P334WT are under LAN side of ZW5)
After change step1 to step2, PC1 and PC2 can reach ZyWALL 5, but can't ping each other.
6. [BUG FIXED]
SPR: 040923929
Symptom: In SMT menu 1, DNS server has unnecessary selection item: Private DNS.
7. [BUG FIXED]
SPR: 050202082
Symptom: Subnet mask error.
Condition:
 - a. If set the IP address to 0.0.0.0, the subnet mask will change to 255.0.0.0
 - b. Then change the subnet mask to 0.0.0.0, the pop-up dialog-box display "subnet mask error".
8. [BUG FIXED]
SPR: 040923910
Symptom: DUT will crash after run Ethernet stress test by LeapFTP
9. [BUG FIXED]
SPR: 041028867
Symptom: Station can't connect with DUT with heavy traffic.
10. [FEATURE CHANGED]
SPR: 050408255, 050411283
Symptom: Remove Route selection on GUI and metric field on GUI/SMT for Traffic Redirect function.
11. [FEATURE CHANGED]
Symptom: Remove NAT full feature on GUI, but keep full feature in SMT for backward compatible.
12. [BUG FIXED]
SPR: 050428396
Symptom: WLAN STA can't ping to gateway
Condition: Topology is as follows :PC))) P334-----G1000
 - 1). PC connects to P334 WT by wirelessfirst
 - 2). PC switch wireless connection to G1000
 - 3). PC can not get IP if switch to G1000 neither ping to gateway (P334WT)

Modification in 3.60(JN.5)C0 | 05/16/2005

ZyXEL Confidential

Convert version string from "3.60(JN.5)b2" to "3.60(JN.5)"

Modification in 3.60(JN.5)b2 | 05/13/2005

1. [BUG FIXED]
SPR: 050511610
Symptom:
WLAN association list on GUI display error.
Condition:
WLAN association list on GUI display error.

Modification in 3.60(JN.5)b1 | 05/09/2005

1. [FEATURE CHANGED]
Media bandwidth management for SIP still works even though ALG_SIP is disable
2. [FEATURE ENHANCED]
ALG enable/disable setting can be saved in rom file.
3. [FEATURE CHANGED]
Name Modified:
ALG_MSMN -->ALG_MSNM
ALG_VOIP -->ALG_H323

Modification in 3.60(JN.4)C0 | 04/13/2005

Convert version string from "3.60(JN.4)b3" to "3.60(JN.4)"

Modification in V3.60(JN.4)b3 | 04/02/2005

1. [BUG FIXED]
SPR: 050329422
Symptom: Static route for WAN subnet mask has some problem.
Condition:
1). Set WAN Encapsulation to Ethernet/ Dynamic IP.
2). Add static route on WAN, then check the route added to routing table.
3). Reboot system and make sure the WAN get IP again, then check the routing table, the route is not exist
2. [BUG FIXED]
SPR: 050329425
Symptom: BWM configure problem use wizard setup
Condition :
1. In eWC->Wizard->Bandwidth Setup
2. Active managed bandwidth->select bandwidth managed service is WWW
->finish BWM setup Goto Bandwidth MGMT click Apply button =>Fail,status show "Failure to operate setting! Error code = 15 "

Modification in V3.60(JN.4)b2 | 03/23/2005

1. [BUG FIXED]

ZyXEL Confidential

Symptom: When two STAs connected to P-334WT, then move one, in eWC, MAINTENANCE, Association List can not refresh.

Condition:

1. Use G-100 & B-220 to connect with P-334WT.
 2. Into eWC-> MAINTENANCE-> Association List, you can see two station (G-100 & B-220) in here.
 3. Remove B-220.
 4. Click refresh button, B-220 station is still displayed in this page. This is incorrect.
2. [BUG FIXED]

Symptom: WLAN association list work Fail.

Condition:

In eWC / Maintenance / Association List

- a. The list display error MAC address .
 - b. Sometimes it can't display the MAC address.
3. [BUG FIXED]

Symptom: When users remotely manage the ZyWALL via a PPTP connection, a strange firewall session (between PPTP server and PPTP client) timeout log may be observed.

Condition:

1. Configure the ZyWALL's WAN port to use PPTP encapsulation.
 2. Remotely login eWC (http/https) via the PPTP connection.
 3. After a few minutes, check the centralized logs or syslogs, you will observe a sequence of firewall logs of http/https session timeout.
4. [FEATURE ENHANCED]

Symptom: The PPTP connection between a ZyXEL router and a Thomson SpeedTouch DSL modem may be reset after the ZyXEL router transmits a _large_quantity_ of packets.

Condition:

1. Connect a ZyXEL router to a Thomson SpeedTouch DSL modem.
 2. Configure the router to establish a PPTP connection to the modem.
 3. Have the router transmit a _large_quantity_ of packets via the modem.
 4. Observe STM 24.1 for any sign of PPTP disconnection. (The PPTP connection suffers a risk of drop for around every 65536 packets transmitted by the router.)
5. [FEATURE ENHANCED]

Add following Time Zone:

GMT-3:30 Newfoundland

GMT+3:30 Tehran

GMT+4:30 Kabul

GMT+5:30 Bornbay, Calcutta, Madras, New Delhi

GMT+5:45 Katmandu

GMT+6:30 Yangon

GMT+9:30 Adelaide, Darwin.

6. [FEATURE CHANGED]

Change username length of PPPoE and PPTP to 62

7. [FEATURE ENHANCED]

Merge Genie functionality into this version

Modification in 3.60(JN.4)b1 | 01/26/2005

1. [BUG FIXED]
Symptom: Wireless Static Web can't configure.
Condition:
 1. On eWC Wireless page, select Static WEB and Passphrase is empty then click Generate button
 2. Status will show "Please Input Passphrase" and Security select No Security and click Apply, Status will show this message again and can't not save.
2. [BUG FIXED]
Symptom: In eWC Remote Management, if you select DNS tab, then you can not move to TELNET tab.
Condition:
Into eWC-> Remote Management-> DNS page, You can't go to TELNET page from this page.
3. [BUG FIXED]
Symptom: When two STAs connected to P-334WT, then move one, in eWC, MAINTENANCE, Association List can not refresh.
Condition:
 1. Use G-100 & B-220 to connect with P-334WT.
 2. Into eWC-> MAINTENANCE-> Association List, you can see two station (G-100 & B-220) in here.
 3. Remove B-220.
 4. Click refresh button, B-220 station is still displayed in this page. This is incorrect.
4. [BUG FIXED]
Symptom: Bandwidth Management problem.
Condition:
Under Bandwidth Management, the managed traffic will be processed one-by-one instead of concurrently processing if they are configured as the same priority.
5. [FEATURE ENHANCED]
SMTP Authentication
6. [FEATURE ENHANCED]
OTIST LED Support
7. [FEATURE ENHANCED]
WLAN MAC Spoofing

Modification in 3.60(JN.3)C0 | 12/15/2004

Convert version string from "3.60(JN.3)b1" to "3.60(JN.3)"

Modification in 3.60(JN.3)b1 | 12/15/2004

No external changes.

Modification in 3.60(JN.2)D0 | 12/13/2004

Change NAT timeout to 180 seconds.

Convert version string from "3.60(JN.2)b1" to "3.60(JN.2)"

Modification in 3.60(JN.2)C0 | 12/13/2004

Convert version string from "3.60(JN.2)b1" to "3.60(JN.2)"

Modification in 3.60(JN.2)b1 | 12/09/2004

1. [BUG FIXED]
Symptom: Apply call schedule rule to WAN ,DUT will crash
Condition: 1.Set WAN encapsulation is PPPoE
2. Edit a schedule rule name is 1
3.Goto SMT Menu 11 , Set schedules=1 then save to rom
=>DUT will crash while PPPoE is trigger.
2. [BUG FIXED]
Symptom: System exception and reboot occur when system name is up to 30 characters long and enable 802.1x.
Condition:
1. Set SMT menu 1 System Name more then 16 characters.
2. enable 802.1x or WPA.
3. user association.
4. system exception.
3. [BUG FIXED]
MAC Filter page, if we input invalid MAC data, the error message shows "Invalid MAC Address #4".
4. [FEATURE CHANGED]
Symptom: The GUI arrangement for content filter.
Condition: eWC-> Content filter, Wish Monday ~ Sunday can be listed on the same line.
5. [BUG FIXED]
Symptom: IP alias configure problem
Condition: 1.In eWC configure IP alias
2.Set IP alias 1 IP is same as alias 2 =>Fail ,no error message and it still can save to ROM.
6. [BUG FIXED]
Symptom: Refresh button don't work.
Condition: 1). Establish a VPN tunnel.
2). eWC-> VPN-> SA Monitor, You can see a VPN tunnel display on this page. (don't leave this page)
3). Drop the VPN tunnel, then Establish it again.
4). Continue step 2, click the Refresh button, The VPN tunnel can't display again.
7. [FEATURE CHANGED]
WAN page naming problem in Chinese version GUI. Change "外部網路" to "廣域網路".

ZyXEL Confidential

8. [FEATURE CHANGED]
Change eWC string from “OTIST in Process” to “OTIST in Progress”.
9. [BUG FIXED]
The OTIST setup key will be overwritten by “01234567” after reboot if user keeps key empty.
10. [FEATURE CHANGED]
In System -> IP Alias page, only alias1 and alias2 are active, IP address 1 and 2 must be check.
11. [BUG FIXED]
Symptom: G-405 (or P2000W) can't get IP from P-334WT.
Condition: Turn bandwidth management on (I used VoIP and WWW via the bandwidth wizard), and the G-405 (or P2000W) can not pull a DHCP address. Turn off bandwidth management, and the G-405 (or P2000W) has no problem pulling an address.
12. [BUG FIXED]
Symptom: Parental Control always disabled by license control.
Condition:
 1. Enable TMSS and Parental Control.
 2. Active your account on Dashboard of TMSS.
 3. Wait a period, Parental Control still disabled by license control. It should be enabled.
13. [FEATURE CHANGED]
Rearrange the order in eWC maintenance statistics page.

Modification in 3.60(JN.1)D0 | 11/19/2004

Change NAT timeout to 180 seconds.

Convert version string from "3.60(JN.1)b1" to "3.60(JN.1)"

Modification in 3.60(JN.1)C0 | 11/19/2004

Convert version string from "3.60(JN.1)b1" to "3.60(JN.1)"

Modification in 3.60(JN.1)b1 | 11/09/2004

4. [BUG FIXED]
Symptom: P2002 (P2P) SIP pass through test fail.
Condition: P2002_1-----P-334WT_1-----P-334WT_2----- P2002_2
 1. Phone call setting is P2P.
 2. Set default server to P2002.
 3. P2002_2 can't receive P2002_1's Ring.
5. [BUG FIXED]
Symptom: GUI's problem for VPN's configuration.
Condition: eWC-> ADVANCED->VPN ->Rule Setup,"Security Gateway Address" can not type in a domain name.
6. [BUG FIXED]

ZyXEL Confidential

Symptom: Can't into OTIST's Process if none Setup Key.

Condition: 1). eWC-> ADVANCED->WIRELESS ->OTIST, make key value of Setup Key to blank.

2). eWC-> ADVANCED->WIRELESS ->OTIST, click "Start" button.

==> eWC display "Please input key value."

7. [BUG FIXED]

Symptom: Wireless has some problem.

Condition: 1). Change wireless security type from WPA-PSK to Static WEP.

2). Use AiroPeek to capture, P-334WT's security type is still WPA-PSK.

Modification in 3.60(JN.0)C0 | 10/29/2004

Convert version string from "3.60(JN.0)b4" to "3.60(JN.0)"

TMSS Dashboard URL is <http://tmss.trendmicro.com/dashboard>

Modification in 3.60(JN.0)b4 | 10/27/2004

1. [FEATURE CHANGED]

Change the system name from "P334WT" to "P-334WT"

2. [FEATURE CHANGED]

Change string from "Auto Security in Process" to "OTIST in Process" when OTIST starts in GUI

3. [FEATURE CHANGED]

Change string from "One-touch Intelligent Security" to "One-Touch Intelligent Security" in GUI

4. [BUG FIXED]

Symptom: Cannot access Dashboard correctly.

Condition: 1. Set you dashboard URL to beta.tmss.trendmicro.com.

2. Connect to tmss.trendmicro.com directly.

3. Browser will display message "you need a Trend Micro-approved router to connect to the Internet".

5. [BUG FIXED]

Symptom: Can't display full message on popup window.

Condition: 1). Set wireless security to Static WEP/ 256 Bits/ Hex.

2). eWC-> Wireless LAN-> OTIST, push START button.

3). Popup a window to display the setting value of wireless security, but not display full word for the 256 Bits WEP key.

6. [BUG FIXED]

The red light on the right front side of the unit turns on when host connect to LAN 3.

7. [BUG FIXED]

Condition: 1). Restore default rom file.

2). eWC-> Wizard, the default Domain Name = zyxel.com.tw. The field should be empty.

Modification in 3.60(JN.0)b3 | 10/15/2004

1. [BUG FIX]
Change the redirect URL of TMSS from IP to domain name.
2. [FEATURE CHANGED]
Focus the cursor at Password field in login page.
3. [FEATURE CHANGED]
Refine the eWC string from “SYS” to “PWR” in firmware upgrade page.
4. [FEATURE CHANGED]
Add scroll bar on eWC panel.
5. [BUG FIX]
After configuring 128-bit WEP and performing some tests yesterday, I changed the wireless configuration to WPA-PSK. This morning I changed the configuration to static WEP. The screen displayed 64-bit WEP and the keys were truncated to 64 bits. The 128-bit WEP information should be remembered.
6. [BUG FIX]
Model name show P660HW not P-334WT in Dashboard.
7. [BUG FIX]
Symptom: The ”Reset” button of Back to Factory Defaults is unavailable.
Condition: eWC-> MAINTENANCE-> Configuration, IE displayed ”網頁發生錯誤” after click ”Reset” button.
8. [FEATURE CHANGED]
With the screen set to 800x600 pixels, the user cannot see or reach all of the menu options, unless the menu options are limited to the major menu items. For example, if Advanced is open, the user cannot see the Maintenance or Logout options. The present design assumes everyone will use 1024x768 pixels, or higher.
9. [BUG FIX]
Symptom: WPA Mixed mode fail.
Condition: 1). One station run WPA (TLS).
2). the other one run 802.1x-TLS (Dynamic 64/128 WEP), can’t connect with DUT.
10. [BUG FIX]
Symptom: DUT reboots by H/W watch dog.
Condition: 1). eWC-> wireless, disable Wireless LAN, Apply.
2). Enable Wireless LAN, Apply.
3). disable G+ Enhanced then change RTS/CTS Threshold & Fragmentation Threshold to 2432, Apply.
The Setting can’t save to rom and DUT reboots by H/W watch dog.
11. [BUG FIX]
When I disable wireless LAN, the WLAN light turns off, but the site is still visible in a site survey on two laptops.
12. [BUG FIX]
Symptom: Rom file damaged.
Condition: 1). eWC-> Firewall-> Services, add FTP(TCP:20,21) to Blocked Services, Apply.
2). eWC-> Firewall-> Services, delete FTP(TCP:20,21) from Blocked Services, Apply.
3). Reboot DUT, DUT will do crash dump cycle.

13. [BUG FIX]
Symptom: Configuration problem of BM.
Condition: 1). eWC-> Bandwidth Management, add rule one, Apply.
2). eWC-> Bandwidth Management-> Select rule one-> Edit, not change anything, Apply. Can't save again that display "Destination IP format error !".
14. [BUG FIX]
Symptom: Bandwidth management problem
Condition: 1.Edit bandwidth management rule for FTP/WWW/Mail
2.Generate FTP/WWW/Mail package by chariot
3.Monitor bandwidth usage status =>Fail, bandwidth usage not correct
15. [BUG FIX]
Use Smartbit test throughput are lower than V3.60(JN.0)b1.
16. [BUG FIX]
Symptom: DUT crash.
Condition: 1). Set WAN to PPTP mode.
2). Spoof MAC address of LAN IP.
3). First & second times happened : access support SSL's web site.
Third times happened : Access internet web site and poop up TMSS's Dashboard.
Exception occurred!
EPC= 0x8009E5D0
SR= 0x00000003
CR= 0x9080840C
\$RA= 0x00000000
TLBS..\src\sys_isr.c:489 sysreset()
17. [BUG FIX]
Symptom: DUT will crash after run FTP stress test.
Condition: 1). WAN Encapsulation set to PPTP mode.
2). One host use FTP download file overnight by wireless.
3). One host use FTP download file overnight by wire.
Exception occurred!
EPC= 0x800A88D0
SR= 0x00000003
CR= 0x90808414
\$RA= 0x00000000
AdES ..\src\sys_isr.c:489 sysreset()

Modification in 3.60(JN.0)b2 | 10/01/2004

18. [BUG FIX]
Symptom: ICMP packet cannot response.
Condition: 1. Enable Firewall and set default SUA server to a exist host.
2. ICMP packet would be blocked by Firewall.
19. [BUG FIX]
Symptom & Condition: Buttons of multi language cannot work when using Mozilla login.

20. [BUG FIX]
Symptom: Display error in parental control.
Condition: 1. Active parental control.
2. After a period time.
3. In eWC->TMSS->Parental Control, has "0.0.0.0" displayed in address list.
21. [FEATURE CHANGED]
Change the redirect URL of TMSS from IP to domain name.
22. [FEATURE ENHANCED]
Support multi language for blocking page of Parental Control.
23. [BUG FIX]
Symptom: System crash.
Condition: 1. Enable TMSS->Parental Control.
2. Connect to Internet and router would crash sometimes.
24. [FEATURE ENHANCED]
Router will trigger license check if client active register at dashboard.
25. [BUG FIX]
Symptom & Condition: Trend Micro Internet Security 2005 cannot display correctly at eWC.
26. [BUG FIX]
Symptom: Sometimes router reboots by software watchdog.
Condition: 1. Put router on the network for a long time.
2. Sometimes router will reboot by software watchdog.
27. [FEATURE CHANGED]
When enable/disable Trend Micro Security Services at Service Settings, router will also enable/disable Automatically update and parental control.
28. [BUG FIX]
Symptom: Script error occurs when setting static IP via Wizard Setup.
Condition: 1. Turn on IE's script error notification.
2. Setup static IP via Wizard Setup.
3. Script error occurs when clicking the "Next" button.
29. [BUG FIX]
Symptom & Condition: Html code is displayed on the Parental Control blocking page.
30. [FEATURE CHANGED]
Remove SMT14 Dial-in User Setup. In SMT23.4, no local user database available anymore in Authentication Databases.
31. [BUG FIX]
Use Mozilla login, buttons of Multi language can't work on home page.
32. [BUG FIX]
Symptom: DUT crash while click DHCP Table.
Condition: 1). Set LAN DHCP server= None.
2). Check host can ping DUT's LAN by static IP.
3). eWC-> MAINTENANCE, If click DHCP Table that will be occurred DUT crash.
33. [BUG FIX]
Symptom: Can't save PPTP to static IP by Wizard configuration
Condition: 1). eWC-> Connection Wizard 2, change Encapsulation to PPTP.

- 2). eWC-> Connection Wizard 3, select "Use fixed IP address" and set My WAN IP Address, Apply.
- 3). Screen display "Error: Subnet Mask format error."
34. [BUG FIX]
Symptom: In eWC VPN SA monitor not show active VPN rule.
Condition: In eWC VPN SA monitor not show active VPN rule when VPN tunnel is establish.
35. [BUG FIX]
Symptom: Bandwidth management problem
Condition: 1.Edit bandwidth management rule for FTP/WWW/Mail
2.Generate FTP/WWW/Mail package by chariot
3.Monitor bandwidth usage status =>Fail, bandwidth usage not correct
36. [BUG FIX]
Symptom: Model name is wrong.
Condition: Model name is P-334WT, not Prestige 334WT. Please modify all model name in system.
37. [BUG FIX]
DUT will crash while test throughput of VPN IKE 3DES by SmartBits.
(Test duration set to 60 sec).
38. [BUG FIX]
Symptom: Can't access Java web.
Condition: 1). eWC-> CONTENT FILTER, enable block Cookies.
2). Can't access Java web: <http://java.sun.com/applets/>.
39. [BUG FIX]
Symptom: GUI's problem for VPN's configuration.
Condition: eWC-> ADVANCED->VPN ->Rule Setup,VPN configuration can't save to rom if Local-content-IP is none.
40. [BUG FIX]
Symptom: The WLAN's status should be Down when Wireless is disabled.
Condition: 1). Disable Wireless.
2). WLAN's status still displayed 54M in menu 24.1.
41. [BUG FIX]
Symptom: Wireless is unstable with G-100, the connection is easy to drop.
Condition: 1). Host use G-100 to connect with P-334WT (no security).
2). The connection is easy to drop while download file.
42. [BUG FIX]
Symptom: DUT reboot after run eMule.
Condition: 1). Set WAN Encapsulation to Ethernet/ Dynamic IP.
2). Set forwarding 4661 ~ 4662 port to host.
3). Host run eMule about 2 hours, DUT reboot.
43. [BUG FIX]
Symptom: DUT do reboot cycle
Condition: 1). Continue SPR 40923908.
2). Run eMule & access internet web about 3 hours, DUT do reboot cycle.
44. [BUG FIX]
Symptom: Has different subnet mask IP display in DHCP

Condition: 1). Set a Static DHCP rule for Host_A, and the IP not in range of IP Pool.
(ex, Static DHCP IP set 192.168.1.5, IP Pool starting address: 192.168.1.33)

2). Host_A get 192.168.1.5 IP from DUT.

3). Host_B get 192.168.1.33 IP from DUT.

4). eWC-> MAINTENANCE-> DHCP Table, display "192.168.2.31" IP assign to Host_B.

45. [BUG FIX]

Symptom: DUT always to authenticate with Radius server.

Condition: 1). Set wireless Security to 802.1x+ Static WEP.

2). Set Authentication Databases to Radius-first-then-Local.

3). Set username & password in Local database (MD5).

4). Station can't authenticate MD5 successfully with DUT's Local database, because it only to check Radius server.

46. [BUG FIX]

Symptom: SIP pass through fail.

Condition: P2000W_1-----P-334WT_1-----P-334WT_2----- P2000W_2

1. Phone call setting is Proxy IP.

2. P2000W_2 can't receive P2000W_1's Ring.

47. [BUG FIX]

Symptom: P2002 (Proxy IP) SIP pass through test fail.

Condition: P2002_1-----P-334WT_1-----P-334WT_2----- P2002_2

1. Phone call setting is Proxy IP.

2. P2002_2 can't receive P2002_1's Ring.

48. [BUG FIX]

Symptom: SIP pass through fail

Condition: P2000W_1-----P-334WT_1-----P-334WT_2----- P2000W_2

1. Phone call setting is P2P.

2. Set default server to P2000W.

3. P2000W_2 can't receive P2000W_1's Ring.

49. [BUG FIX]

Symptom: P2002 (P2P) SIP pass through test fail.

Condition: P2002_1-----P-334WT_1-----P-334WT_2----- P2002_2

1. Phone call setting is P2P.

2. Set default server to P2002.

3. P2002_2 can't receive P2002_1's Ring.

50. [BUG FIX]

Symptom: Display error in parental control.

Condition: 1). Active parental control.

2). After a period time.

3). In eWC->TMSS->Parental Control, has "0.0.0.0" displayed in address list.

51. [BUG FIX]

Symptom: DUT didn't response ICMP packet if set default SUA server.

Condition: 1). Set default SUA server to a exist device.

2). Ping WAN IP fail, The ICMP will be blocked for firewall rule.

52. [BUG FIX]

Symptom: AOL 9.0, Live video chat FAIL.

ZyXEL Confidential

Condition: PC_1-----P-334WT_1-----P-334WT_2----- PC_2

1. "Live video chat" can't work.

53. [BUG FIX]

Symptom: Error log problem.

Condition: 1). In menu 24.8, "enter sys log err dis".

2). You will have the result below, by those dump we can see the serial number are not continuous. And the time was automatically add one hour(the actual time=display time - one hour).

1 Thu Sep 23 14:13:15 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

4 Thu Sep 23 14:13:18 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

8 Thu Sep 23 14:13:21 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

12 Thu Sep 23 14:13:24 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

14 Thu Sep 23 14:13:27 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

17 Thu Sep 23 14:13:30 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

18 Thu Sep 23 14:14:45 2004 PP1b WARN Last errorlog repeat 24 Times

20 Thu Sep 23 14:14:45 2004 PP10 WARN netMakeChannDial: err=-3001

rn_p=809de930

21 Thu Sep 23 14:15:33 2004 PP15 WARN Last errorlog repeat 15 Times

54. [BUG FIX]

Symptom: Sometimes P2000W can't get IP from P-334WT.

Condition: 1). Set wireless to no security.

2). Use P2000W association with DUT successfully.

3). Sometimes can get IP from DUT, sometimes can't.

55. [BUG FIX]

Symptom: DUT crash.

Condition: 1). Set WAN to PPTP mode.

2). Spoof MAC address of LAN IP.

3). First & second times happened : access support SSL's web site.

Third times happened : Access internet web site and pop up TMSS's Dashboard.

Exception occurred!

EPC= 0x8009E5D0

SR= 0x00000003

CR= 0x9080840C

\$RA= 0x00000000

TLBS.\src\sys_isr.c:489 sysreset()

Modification in 3.60(JN.0)b1 | 08/31/2004

ZyXEL Confidential

First Firmware Release

Annex A CI Command List

Last Updated: 2002/11/26

| Command Class List Table | | |
|---|--|---|
| System Related Command | Exit Command | Device Related Command |
| Ethernet Related Command | POE Related Command | PPTP Related Command |
| Configuration Related Command | IP Related Command | IPSec Related Command |
| Firewall Related Command | Wireless LAN Related Command | Bridge Related Command |
| Radius Related Command | 802.1x Related Command | Auto WLAN Security Delivery Command |

| System Related Command | | | | Home |
|------------------------|-------------|----------|--|---|
| | Command | | | Description |
| sys | | | | |
| | adjtime | | | retrive date and time from Internet |
| | callhist | | | |
| | | display | | display call history |
| | | remove | <index> | remove entry from call history |
| | countrycode | | [countrycode] | set country code |
| | date | | [year month date] | set/display date |
| | domainname | | | display domain name |
| | edit | | <filename> | edit a text file |
| | extraphnum | | | maintain extra phone numbers for outcalls |
| | | add | <set 1-3> <1 st phone num> [2 nd phone num] | add extra phone numbers |
| | | display | | display extra phone numbers |
| | | node | <num> | set all extend phone number to remote node <num> |
| | | remove | <set 1-3> | remove extra phone numbers |
| | | reset | | reset flag and mask |
| | feature | | | display feature bit |
| | hostname | | [hostname] | display system hostname |
| | logs | | | |
| | | category | | |
| | | | access [0:none/1:log/2:alert/3:both] | record the access control logs |
| | | | attack [0:none/1:log/2:alert/3:both] | record and alert the firewall attack logs |
| | | | display | display the category setting |
| | | | error [0:none/1:log/2:alert/3:both] | record and alert the system error logs |
| | | | ipsec [0:none/1:log/2:alert/3:both] | record the access control logs |
| | | | ike [0:none/1:log/2:alert/3:both] | record the access control logs |
| | | | javablocked [0:none/1:log] | record the java etc. blocked logs |
| | | | mten [0:none/1:log] | record the system maintenance logs |
| | | | upnp [0:none/1:log] | record upnp logs |
| | | | urlblocked [0:none/1:log/2:alert/3:both] | record and alert the web blocked logs |
| | | | urlforward [0:none/1:log] | record web forward logs |
| | | clear | | clear log |
| | | display | [access attack error ipsec ike javablocked mten urlblocked urlforward] | display all logs or specify category logs |
| | | errlog | | |
| | | | clear | display log error |
| | | | disp | clear log error |
| | | | online | turn on/off error log online display |
| | | load | | load the log setting buffer |

ZyXEL Confidential

| | | | | |
|--|-----------|----------|--|---|
| | | mail | | |
| | | | alertAddr [mail address] | send alerts to this mail address |
| | | | display | display mail setting |
| | | | logAddr [mail address] | send logs to this mail address |
| | | | schedule display | display mail schedule |
| | | | schedule hour [0-23] | hour time to send the logs |
| | | | schedule minute [0-59] | minute time to send the logs |
| | | | schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none] | mail schedule policy |
| | | | schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat] | weekly time to send the logs |
| | | | server [domainName/IP] | mail server to send the logs |
| | | | subject [mail subject] | mail subject |
| | | save | | save the log setting buffer |
| | | syslog | | |
| | | | active [0:no/1:yes] | active to enable unix syslog |
| | | | display | display syslog setting |
| | | | facility [Local ID(1-7)] | log the messages to different files |
| | | | server [domainName/IP] | syslog server to send the logs |
| | log | | | |
| | | clear | | clear log error |
| | | disp | | display log error |
| | | online | [on/off] | turn on/off error log online display |
| | | resolve | | Resolve mail server and syslog server address |
| | mbuf | | | |
| | | link | link | list system mbuf link |
| | | pool | <id> [type] | list system mbuf pool |
| | | status | | display system mbuf status |
| | | disp | <address> | display mbuf status |
| | | cnt | | |
| | | | disp | display system mbuf count |
| | | | clear | clear system mbuf count |
| | | debug | [on/off] | |
| | pwderrtm | | [minute] | Set or display the password error blocking timeout value. |
| | rn | | | |
| | | load | <entry no.> | load remote node information |
| | | disp | <entry no.>(0:working buffer) | display remote node information |
| | | nat | <none sua full_feature> | config remote node nat |
| | | nailup | <no yes> | config remote node nailup |
| | | mtu | <value> | set remote node mtu |
| | | save | [entry no.] | save remote node information |
| | smt | | | not support in this product |
| | stdio | | [minute] | change terminal timeout value |
| | time | | [hour [min [sec]]] | display/set system time |
| | treisp | | | monitor packets |
| | trelog | | | |
| | trepacket | | | |
| | syslog | | | |
| | | server | [destIP] | set syslog server IP address |
| | | facility | <FacilityNo> | set syslog facility |
| | | type | [type] | set/display syslog type flag |

ZyXEL Confidential

| | | | |
|------------|----------|--|---|
| | mode | [on/off] | set syslog mode |
| version | | | display RAS code and driver version |
| view | | <filename> | view a text file |
| wdog | | | |
| | switch | [on/off] | set on/off wdog |
| | cnt | [value] | display watchdog counts value: 0-34463 |
| romreset | | | restore default romfile |
| server | | | |
| | access | <telnet ftp web icmp snmp dns> <value> | set server access type |
| | load | | load server information |
| | disp | | display server information |
| | port | <telnet ftp web snmp> <port> | set server port |
| | save | | save server information |
| | secureip | <telnet ftp web icmp snmp dns> <ip> | set server secure ip addr |
| fwnotify | | | |
| | load | | load fwnotify entry from spt |
| | save | | save fwnotify entry to spt |
| | url | <url> | set fwnotify url |
| | days | <days> | set fwnotify days |
| | active | <flag> | turn on/off fwnotify flag |
| | disp | | display firmware notify information |
| | check | | check firmware notify event |
| | debug | <flag> | turn on/off firmware notify debug flag |
| cmgr | | | |
| | trace | | |
| | | disp <ch-name> | show the connection trace of this channel |
| | | clear <ch-name> | clear the connection trace of this channel |
| | cnt | <ch-name> | show channel connection related counter |
| socket | | | display system socket information |
| filter | | | |
| | netbios | | |
| roadrunner | | | |
| | debug | <level> | enable/disable roadrunner service 0: diable <default> 1: enable |
| | display | <iface name> | display roadrunner information iface-name: enif0, wanif0 |
| | restart | <iface name> | restart roadrunner |
| ddns | | | |
| | debug | <level> | enable/disable ddns service |
| | display | <iface name> | display ddns information |
| | restart | <iface name> | restart ddns |
| | logout | <iface name> | logout ddns |
| cpu | | | |
| | display | | display CPU utilization |
| filter | | | |
| | netbios | | |
| upnp | | | |
| | active | [0:no/1:yes] | Activate or deactivate the saved upnp settings |
| | config | [0:deny/1:permit] | Allow users to make configuration changes. through UPnP |
| | display | | display upnp information |
| | firewall | [0:deny/1:pass] | Allow UPnP to pass through Firewall. |
| | load | | save upnp information |

ZyXEL Confidential

| | | | | |
|--|--|------|--|-----------------------|
| | | save | | save upnp information |
|--|--|------|--|-----------------------|

Exit Command

[Home](#)

| Command | | | | Description |
|---------|--|--|--|---------------|
| exit | | | | exit smt menu |

Device Related Command

[Home](#)

| Command | | | | Description |
|---------|---------|------|----------------|---------------------|
| dev | | | | |
| | channel | | | |
| | | drop | <channel name> | drop channel |
| | dial | | <node#> | dial to remote node |

Ethernet Related Command

[Home](#)

| Command | | | | Description |
|---------|---------|-------------|----------------------|--|
| ether | | | | |
| | config | | | display LAN configuration information |
| | driver | | | |
| | | cnt | | |
| | | | disp <name> | display ether driver counters |
| | | ioctl | <ch_name> | Useless in this stage. |
| | | status | <ch_name> | see LAN status |
| | version | | | see ethernet device type |
| | pkttest | | | |
| | | disp | | |
| | | | packet <level> | set ether test packet display level |
| | | | event <ch> [on/off] | turn on/off ether test event display |
| | | sap | [ch_name] | send sap packet |
| | | arp | <ch_name> <ip-addr> | send arp packet to ip-addr |
| | debug | | | |
| | | disp | <ch_name> | display ethernet debug infomation |
| | | level | <ch_name> <level> | set the ethernet debug level level 0: disable debug log level 1:enable debug log (default) |
| | edit | | | |
| | | load | <ether no.> | load ether data from spt |
| | | mtu | <value> | set ether data mtu |
| | | accessblock | <0:disable 1:enable> | block internet access |
| | | save | | save ether data to spt |

POE Related Command

[Home](#)

| Command | | | | Description |
|---------|--------|--|-----------|-------------------------------|
| poe | | | | |
| | status | | [ch_name] | see poe status |
| | dial | | <node> | dial a remote node |
| | drop | | <node> | drop a pppoe call |
| | ether | | [rfc3com] | set /display pppoe ether type |

PPTP Related Command

[Home](#)

| Command | | | | Description |
|---------|--------|--|-------------|---------------------------------|
| pptp | | | | |
| | dial | | <rn-name> | dial a remote node |
| | drop | | <rn-name> | drop a remote node call |
| | tunnel | | <tunnel id> | display pptp tunnel information |

Configuration Related Command

[Home](#)

| Command | | | | | Description |
|----------|----------|--------------------|--|--|---|
| config | | | | | The parameters of config are listed below. |
| edit | firewall | active <yes/no> | | | Activate or deactivate the saved firewall settings |
| retrieve | firewall | | | | Retrieve current saved firewall settings |
| save | firewall | | | | Save the current firewall settings |
| display | firewall | | | | Displays all the firewall settings |
| | | set <set#> | | | Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set. |
| | | set <set#> | rule <rule#> | | Display current entries of a rule in a set. |
| | | attack | | | Display all the attack alert settings in PNC |
| | | e-mail | | | Display all the e-mail settings in PNC |
| | | ? | | | Display all the available sub commands |
| | | e-mail | mail-server <mail server IP> | | Edit the mail server IP to send the alert |
| | | | return-addr <e-mail address> | | Edit the mail address for returning an email alert |
| | | | e-mail-to <e-mail address> | | Edit the mail address to send the alert |
| | | | policy <full hourly daily weekly> | | Edit email schedule when log is full or per hour, day, week. |
| | | | day <sunday monday tuesday wednesday thursday friday saturday> | | Edit the day to send the log when the email policy is set to Weekly |
| | | | hour <0~23> | | Edit the hour to send the log when the email policy is set to daily or weekly |
| | | | minute <0~59> | | Edit the minute to send to log when the email policy is set to daily or weekly |
| | | | Subject <mail subject> | | Edit the email subject |
| | | attack | send-alert <yes/no> | | Activate or deactivate the firewall DoS attacks notification emails |
| | | | block <yes/no> | | Yes: Block the traffic when exceeds the tcp-max-incomplete threshold |
| | | | | | No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold |
| | | | block-minute <0~255> | | Only valid when sets 'Block' to yes. The unit is minute |
| | | | minute-high <0~255> | | The threshold to start to delete the old half-opened sessions to minute-low |
| | | | minute-low <0~255> | | The threshold to stop deleting the old half-opened session |
| | | | max-incomplete-high <0~255> | | The threshold to start to delete the old half-opened sessions to max-incomplete-low |
| | | | max-incomplete-low <0~255> | | The threshold to stop deleting the half-opened session |
| | | | tcp-max-incomplete ete <0~255> | | The threshold to start executing the block field |

ZyXEL Confidential

| | | | | | |
|--|--|------------|--------------------------------|--|--|
| | | set <set#> | name <desired name> | | Edit the name for a set |
| | | | default-permit <forward block> | | Edit whether a packet is dropped or allowed when it does not match the default set |
| | | | icmp-timeout <seconds> | | Edit the timeout for an idle ICMP session before it is terminated |
| | | | udp-idle-timeout <seconds> | | Edit the timeout for an idle UDP session before it is terminated |
| | | | connection-timeout <seconds> | | Edit the wait time for the SYN TCP sessions before it is terminated |
| | | | fin-wait-timeout <seconds> | | Edit the wait time for FIN in concluding a TCP session before it is terminated |
| | | | tcp-idle-timeout <seconds> | | Edit the timeout for an idle TCP session before it is terminated |
| | | | pnc <yes no> | | PNC is allowed when 'yes' is set even there is a rule to block PNC |
| | | | log <yes no> | | Switch on/off sending the log for matching the default permit |
| | | | rule <rule#> | permit <forward block> | Edit whether a packet is dropped or allowed when it matches this rule |
| | | | | active <yes no> | Edit whether a rule is enabled or not |
| | | | | protocol <0~255> | Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP... |
| | | | | log <none match not-match both> | Sending a log for a rule when the packet none matches not match both the rule |
| | | | | alert <yes no> | Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert. |
| | | | | srcaddr-single <ip address> | Select and edit a source address of a packet which complies to this rule |
| | | | | srcaddr-subnet <ip address> <subnet mask> | Select and edit a source address and subnet mask if a packet which complies to this rule. |
| | | | | srcaddr-range <start ip address> <end ip address> | Select and edit a source address range of a packet which complies to this rule. |
| | | | | destaddr-single <ip address> | Select and edit a destination address of a packet which complies to this rule |
| | | | | destaddr-subnet <ip address> <subnet mask> | Select and edit a destination address and subnet mask if a packet which complies to this rule. |
| | | | | destaddr-range <start ip address> <end ip address> | Select and edit a destination address range of a packet which complies to this rule. |
| | | | | tcp destport-single <port#> | Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers. |
| | | | | tcp destport-range <start port#> <end port#> | Select and edit a destination port range of a packet which comply to this rule. |
| | | | | udp destport-single <port#> | Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers. |
| | | | | udp destport-range <start port#> <end port#> | Select and edit a destination port range of a packet which comply to this rule. |

ZyXEL Confidential

| | | | | | |
|--------|----------|------------|--------------|---|--|
| | | | | desport-custom <desired custom port name> | Type in the desired custom port name |
| delete | firewall | e-mail | | | Remove all email alert settings |
| | | attack | | | Reset all alert settings to defaults |
| | | set <set#> | | | Remove a specified set from the firewall configuration |
| | | set <set#> | rule <rule#> | | Remove a specified rule in a set from the firewall configuration |
| insert | firewall | e-mail | | | Insert email alert settings |
| | | attack | | | Insert attack alert settings |
| | | set <set#> | | | Insert a specified rule set to the firewall configuration |
| | | set <set#> | rule <rule#> | | Insert a specified rule in a set to the firewall configuration |
| cli | | | | | Display the choices of command list. |
| debug | <1 0> | | | | Turn on/off trace for firewall debug information. |

Wireless LAN Related Command

[Home](#)

| Command | | | | Description |
|---------|-------------|--|--------------|----------------------------------|
| wlan | | | | |
| | active | | [on off] | set on/off wlan |
| | association | | | display association list |
| | chid | | [channel id] | set channel |
| | diagnose | | | self-diagnostics |
| | essid | | [ess id] | set ESS ID |
| | version | | | display WLAN version information |

Bridge Related Command

[Home](#)

| Command | | | | Description |
|---------|------|-------|--|---|
| Bridge | | | | |
| | cnt | | | related to bridge routing statistic table |
| | | Disp | | display bridge route counter |
| | | Clear | | clear bridge route counter |
| | stat | | | related to bridge packet statistic table |
| | | Disp | | display bridge route packet counter |
| | | Clear | | clear bridge route packet counter |

Radius Related Command

[Home](#)

| Command | | | | Description |
|---------|------|--|--|---|
| Radius | | | | |
| | auth | | | show current radius authentication server configuration |
| | acct | | | show current radius accounting server configuration |

802.1x Related Command

[Home](#)

| Command | | | | Description |
|---------|-------|-------|---------------|--|
| 8021x | | | | |
| | debug | Level | [debug level] | set ieee802.1x debug message level |
| | | Trace | | show all supplications in the supplication table |
| | | User | [username] | show the specified user status in the supplicant table |

IP Related Command

[Home](#)

ZyXEL Confidential

| Command | | | | Description |
|---------|------------|------------|--|---|
| ip | | | | |
| | address | | [addr] | display host ip address |
| | alias | | <iface> | alias iface |
| | aliasdis | | <0 1> | disable alias |
| | arp | | | |
| | | status | <iface> | display ip arp status |
| | dhcp | | <iface> | |
| | | client | | |
| | | | release | release DHCP client IP |
| | | | renew | renew DHCP client IP |
| | | status | [option] | show dhcp status |
| | dns | | | |
| | | query | | |
| | | server | <primary> [secondary] [third] | set dns server |
| | | stats | | |
| | | | clear | clear dns statistics |
| | | | disp | display dns statistics |
| | httpd | | | |
| | icmp | | | |
| | | status | | display icmp statistic counter |
| | | discovery | <iface> [on off] | set icmp router discovery flag |
| | ifconfig | | [iface] [ipaddr] [broadcast <addr> mtu <value> dynamic] | configure network interface |
| | ping | | <hostid> | ping remote host |
| | route | | | |
| | | status | [if] | display routing table |
| | | add | <dest_addr default>[/<bits>] <gateway> [<metric>] | add route |
| | | addiface | <dest_addr default>[/<bits>] <gateway> [<metric>] | add an entry to the routing table to iface |
| | | addprivate | <dest_addr default>[/<bits>] <gateway> [<metric>] | add private route |
| | | drop | <host addr> [/<bits>] | drop a route |
| | smtp | | | |
| | status | | | display ip statistic counters |
| | stroute | | | |
| | | display | [rule # buf] | display rule index or detail message in rule. |
| | | load | <rule #> | load static route rule in buffer |
| | | save | | save rule from buffer to spt. |
| | | config | | |
| | | | name <site name> | set name for static route. |
| | | | destination <dest addr>[/<bits>] <gateway> [<metric>] | set static route destination address and gateway. |
| | | | mask <IP subnet mask> | set static route subnet mask. |
| | | | gateway <IP address> | set static route gateway address. |
| | | | metric <metric #> | set static route metric number. |
| | | | private <yes no> | set private mode. |
| | | | active <yes no> | set static route rule enable or disable. |
| | traceroute | | <host> [ttl] [wait] [queries] | send probes to trace route of a remote host |
| | xparent | | | |
| | | join | <iface1> [<iface2>] | join iface2 to iface1 group |
| | | break | <iface> | break iface to leave ipxparent group |
| | ave | | | anti-virus enforce |

ZyXEL Confidential

| | | | | |
|--|-----------|----------------|---|--|
| | urlfilter | | | |
| | | reginfo | | |
| | | | display | display urlfilter registration information |
| | | | name | set urlfilter registration name |
| | | | eMail <size> | set urlfilter registration email addr |
| | | | country <size> | set urlfilter registration country |
| | | | clearAll | clear urlfilter register information |
| | | category | | |
| | | | display | display urlfilter category |
| | | | webFeature [block/nonblock] [activex/java/cookei/webproxy] | block or unblock webfeature |
| | | | logAndBlock [log/logAndBlock] | set log only or log and block |
| | | | blockCategory [block/nonblock] [all/type(1-14)] | block or unblock type |
| | | | timeOfDay [always/hh:mm] [hh:mm] | set block time |
| | | | clearAll | clear all category information |
| | | listUpdate | | |
| | | | display | display listupdate status |
| | | | actionFlags [yes/no] | set listupdate or not |
| | | | scheduleFlag [pending] | set schedule flag |
| | | | dayFlag [pending] | set day flag |
| | | | time [pending] | set time |
| | | | clearAll | clear all listupdate information |
| | | exemptZone | | |
| | | | display | display exemptzone information |
| | | | actionFlags [type(1-3)][enable/disable] | set action flags |
| | | | add [ip1] [ip2] | add exempt range |
| | | | delete [ip1] [ip2] | delete exempt range |
| | | | clearAll | clear exemptzone information |
| | | customize | | |
| | | | display | display customize action flags |
| | | | actionFlags[filterList/disableAllExce ptTrusted/unblockRWFTToTrusted/k eywordBlock/fullPath/caseInsensiti ve/fileName][enable/disable] | set action flags |
| | | | logFlags [type(1-3)][enable/disable] | set log flags |
| | | | add [string] [trust/untrust/keyword] | add url string |
| | | | delete [string] [trust/untrust/keyword] | delete url string |
| | | | clearAll | clear all information |
| | | logDisplay | | display cyber log |
| | | ftplist | | update cyber list data |
| | | listServerIP | <ipaddr> | set list server ip |
| | | listServerName | <name> | set list server name |
| | tredir | | | |
| | | failcount | <count> | set tredir failcount |
| | | partner | <ipaddr> | set tredir partner |
| | | target | <ipaddr> | set tredir target |
| | | timeout | <timeout> | set tredir timeout |
| | | checktime | <period> | set tredir checktime |
| | | active | <on/off> | set tredir active |
| | | save | | save tredir information |
| | | disp | | display tredir information |

| | | | | |
|--|------|------------|--------------------------------------|---|
| | | debug | <value> | set tredir debug value |
| | nat | | | |
| | | server | | |
| | | | disp | display nat server table |
| | | | load <set id> | load nat server information from ROM |
| | | | save | save nat server information to ROM |
| | | | clear <set id> | clear nat server information |
| | | | edit active <yes/no> | set nat server edit active flag |
| | | | edit svrport <start port> [end port] | set nat server server port |
| | | | edit intport <start port> [end port] | set nat server forward port |
| | | | edit remotehost <start ip> [end ip] | set nat server remote host ip |
| | | | edit leasetime [time] | set nat server lease time |
| | | | edit rulename [name] | set nat server rule name |
| | | | edit forwardip [ip] | set nat server server ip |
| | | | edit protocol [protocol id] | set nat server protocol |
| | | | edit clear | clear one rule in the set |
| | | service | | |
| | | | irc [on/off] | turn on/off irc flag |
| | | resetport | | reset all nat server table entries |
| | | incikeport | [on/off] | turn on/off increase ike port flag |
| | igmp | | | |
| | | debug | [level] | set igmp debug level |
| | | forwardall | [on/off] | turn on/off igmp forward to all interfaces flag |
| | | querier | [on/off] | turn on/off igmp stop query flag |
| | | iface | | |
| | | | <iface> grouptm <timeout> | set igmp group timeout |
| | | | <iface> interval <interval> | set igmp query interval |
| | | | <iface> join <group> | join a group on iface |
| | | | <iface> leave <group> | leave a group on iface |
| | | | <iface> query | send query on iface |
| | | | <iface> rsptime [time] | set igmp response time |
| | | | <iface> start | turn on of igmp on iface |
| | | | <iface> stop | turn off of igmp on iface |
| | | | <iface> ttl <threshold> | set ttl threshold |
| | | | <iface> vl compat [on/off] | turn on/off vl compat on iface |
| | | robustness | <num> | set igmp robustness variable |
| | | status | | dump igmp status |
| | pr | | | |

IPSec Related Command

[Home](#)

| Command | | | | Description |
|---------|----------------|-------|----------|--|
| ipsec | | | | |
| | debug | <1 0> | | turn on/off trace for IPsec debug information |
| | ipsec_log_disp | | | show IPsec log, same as menu 27.3 |
| | route | lan | <on/off> | After a packet is IPsec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPsec again. |
| | | | | Remark: Command available since 3.50(WA.3) |
| | | wan | <on/off> | After a packet is IPsec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPsec again. |
| | | | | Remark: Command available since 3.50(WA.3) |
| | show_runtime | sa | | display runtime phase 1 and phase 2 SA information |

ZyXEL Confidential

| | | | | |
|--|--------------|-------------|---------------------------------------|--|
| | | spd | | When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD. |
| | switch | <on/off> | | As long as there exists one active IPsec rule, all packets will run into IPsec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPsec rules, packets will not run IPsec process. |
| | timer | chk_my_ip | <1~3600> | - Adjust timer to check if WAN IP in menu is changed |
| | | | | - Interval is in seconds |
| | | | | - Default is 10 seconds |
| | | | | - 0 is not a valid value |
| | | chk_conn. | <0~255> | - Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it. |
| | | | | - Interval is in minutes |
| | | | | - Default is 2 minutes |
| | | | | - 0 means never timeout |
| | | update_peer | <0~255> | - Adjust auto-timer to update IPsec rules which use domain name as the secure gateway IP. |
| | | | | - Interval is in minutes |
| | | | | - Default is 30 minutes |
| | | | | - 0 means never update |
| | updatePeerIp | | | Remark: Command available since 3.50(WA.3) Force system to update IPsec rules which use domain name as the secure gateway IP right away. |
| | | | | Remark: Command available since 3.50(WA.3) |
| | dial | <rule #> | | Initiate IPsec rule <#> from ZyWALL box |
| | | | | Remark: Command available since 3.50(WA.3) |
| | display | <rule #> | | Display IPsec rule # |
| | remote | key | <string> | I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters. |
| | | switch | <on/off> | Activate or de-activate the secured remote access tunnel. |
| | keep_alive | <rule #> | <on/off> | Set ipsec keep_alive flag |
| | load | <rule #> | | Load ipsec rule |
| | save | | | Save ipsec rules |
| | config | netbios | active <on/off> | Set netbios active flag |
| | | | group <group index1, group index2...> | Set netbios group |
| | | name | <string> | Set rule name |
| | | name | <string> | Set rule name |
| | | keyAlive | <Yes No> | Set keep alive or not |
| | | lcIdType | <0:IP 1:DNS 2:Email> | Set local ID type |
| | | lcIdContent | <string> | Set local ID content |
| | | myIpAddr | <IP address> | Set my IP address |

| | | | | |
|--|--|---------------|---|--|
| | | peerIdType | <0:IP 1:DNS 2:Email> | Set peer ID type |
| | | peerIdContent | <string> | Set peer ID content |
| | | secureGwAddr | <IP address Domain name> | Set secure gateway address or domain name |
| | | protocol | <1:ICMP 6:TCP 17:UDP> | Set protocol |
| | | lcAddrType | <0:single 1:range 2:subnet> | Set local address type |
| | | lcAddrStart | <IP> | Set local start address |
| | | lcAddrEndMask | <IP> | Set local end address or mask |
| | | lcPortStart | <port> | Set local start port |
| | | lcPortEnd | <port> | Set local end port |
| | | rmAddrType | <0:single 1:range 2:subnet> | Set remote address type |
| | | rmAddrStart | <IP> | Set remote start address |
| | | rmAddrEndMask | <IP> | Set remote end address or mask |
| | | rmPortStart | <port> | Set remote start port |
| | | rmPortEnd | <port> | Set remote end port |
| | | antiReplay | <Yes No> | Set anitreplay or not |
| | | keyManage | <0:IKE 1:Manual> | Set key manage |
| | | ike | negotiationMode <0:Main 1:Aggressive> | Set negotiation mode in phase 1 in IKE |
| | | | preShareKey <string> | Set pre shared key in phase 1 in IKE |
| | | | p1EncryAlgo <0:DES 1:3DES> | Set encryption algorithm in phase 1 in IKE |
| | | | p1AuthAlgo <0:MD5 1:SHA1> | Set authentication algorithm in phase 1 in IKE |
| | | | p1SaLifeTime <seconds> | Set sa life time in phase 1 in IKE |
| | | | p1KeyGroup <0:DH1 1:DH2> | Set key group in phase 1 in IKE |
| | | | activeProtocol <0:AH 1:ESP> | Set active protocol in phase 2 in IKE |
| | | | p2EncryAlgo <0:Null 1:DES 2:3DES> | Set encryption algorithm in phase 2 in IKE |
| | | | p2AuthAlgo <0:MD5 1:SHA1> | Set authentication algorithm in phase 2 in IKE |
| | | | p2SaLifeTime <seconds> | Set sa life time in phase 2 in IKE |
| | | | encap <0:Tunnel 1:Transport> | set encapsulation in phase 2 in IKE |
| | | | pfs <0:None 1:DH1 2:DH2> | set pfs in phase 2 in IKE |
| | | manual | activeProtocol <0:AH 1:ESP> | Set active protocol in manual |
| | | manual ah | encap <0:Tunnel 1:Transport> | Set encapsulation in ah in manual |
| | | | spi <decimal> | Set spi in ah in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in ah in manual |
| | | | authKey <string> | Set authentication key in ah in manual |
| | | manual esp | encap <0:Tunnel 1:Transport> | Set encapsulation in esp in manual |
| | | | spi <decimal> | Set spi in esp in manual |
| | | | encryAlgo <0:Null 1:DES 2:3DES> | Set encryption algorithm in esp in manual |
| | | | encryKey <string> | Set encryption key in esp in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in esp in manual |
| | | | authKey <string> | Set authentication key in esp in manual |

Firewall Related Command

[Home](#)

| Command | | | | Description |
|---------|----------|--------|----------|---|
| sys | Firewall | | | |
| | | acl | | |
| | | | disp | Display specific ACL set # rule #, or all ACLs. |
| | | active | <yes/no> | Active firewall or deactivate firewall |
| | | clear | | Clear firewall log |
| | | cnt | | |
| | | | disp | Display firewall log type and count. |
| | | | clear | Clear firewall log count. |

ZyXEL Confidential

| | | | | |
|--|--|-------------|----------|---|
| | | disp | | Display firewall log |
| | | online | | Set firewall log online. |
| | | pktdump | | Dump the 64 bytes of dropped packet by firewall |
| | | update | | Update firewall |
| | | dynamicrule | | |
| | | tcprst | | |
| | | | rst | Set TCP reset sending on/off. |
| | | | rst113 | Set TCP reset sending for port 113 on/off. |
| | | | display | Display TCP reset sending setting. |
| | | icmp | | |
| | | dos | | |
| | | | smtp | Set SMTP DoS defender on/off |
| | | | display | Display SMTP DoS defender setting. |
| | | | ignore | Set if firewall ignore DoS in lan/wan/dmz/wlan |
| | | ignore | | |
| | | | dos | Set if firewall ignore DoS in lan/wan/dmz/wlan |
| | | | triangle | Set if firewall ignore triangle route in lan/wan/dmz/wlan |

Annex A CI Command ListAuto WLAN Security Delivery Related Command

[Home](#)

| Command | | | | Description |
|---------|----------|--|--|---|
| autoSec | Start | | | Start the process of WLAN configuration delivery |
| | Duration | | | Set the delivery process duration time in seconds |
| | Port | | | Set the communication port |
| | key | | | Set the communication encryption key |